ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

VG-1: An Optimistic Algorithm for Internet Security

VANI.N[1], SREELATHA.P.K[2], PARVATHY.S[3]

Assistant professor, Dept of CSE, RYMEC, VTU University, Bellary, India[1]

Assistant professor, Dept of CSE, SVIT, VTU University, Bangalore, India[2]

Assistant professor, Dept of ISE, AMC, VTU University, Bangalore, India[3]

Abstract: The impact of internet security is major role in today's technology. To provide greater security for user data we proposes VG-1 security algorithm. It provides efficient and optimistic encryption and decryption algorithm. This algorithm uses encrypted private keys for generation of cipher text. The length of private key is more than 1024 bits. It identifies all types of attacks performed by attacker such as Brute-force attack, sequence modification, timing modification, content modification, and masquerade. VG-1 provides high security and difficult for attacker to decrypt and identify plain text. It provides greater performance, less delay and very efficient encryption and decryption technique when compared to RSA, DES, AES and tripleDES.

Keywords: Confidentiality, Authentication, data Integrity and Non Repudiation

I. INTRODUCTION

Network Security measures are needed to protect data during data transmission [1]. It provides secure data transmission and provides confidentiality for user data which provides benefit for all transactions of online banks, online business, government, and academic organizations interconnect data processing equipments with a collection of interconnected network is required in internet security[2].X.800 is security architecture for OSI defines symmetric approach. X.800 divides these services into five categories:

- Authentication
- Access control
- Data Confidentiality
- Data Integrity
- Non Repudiation

Authentication provides assurance that communication is authentic. Access control is prevention of unauthorized use of resources. Data confidentiality is used to provide protection of transmitted data from passive attacks. Data Integrity provides assurance that data received are exactly are sent by an authorized entity. NonRepudiation provides protection against denial of service by one of the entity involved in a communication [2]. Many schemes used for encryption and decryptions of cipher text are known as Cryptography [3].The cryptography is characterized along three independent dimensions:

- The number of efficient techniques used for encryption from plaintext to cipher text.
- The number of keys used.
- The number of optimistic and efficient techniques used for decryption from cipher text to plain text.

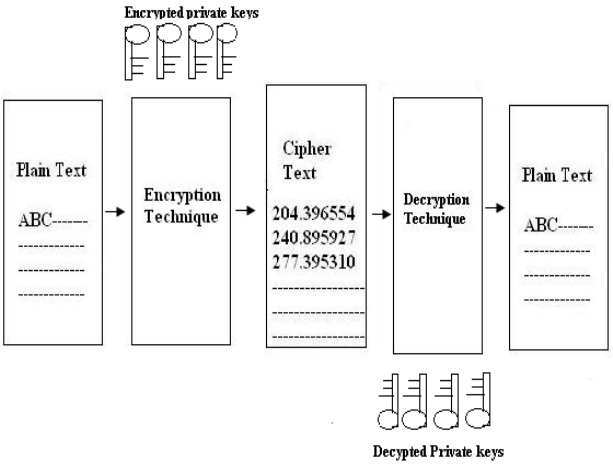

Fig1: VG-1 Cryptography Technique

II. EXISTING SYSTEM

The DES (Data Encryption Standard) Algorithm converts plaintext into cipher text with help of 56 bit secret key. The length of the key is 56 bit may not be sufficient to provide full security [1]. Bluefish algorithm is time consuming on sub key generation process. Bluefish are key dependent. The AES (Advanced Encryption Standard) protocol has better security strength than DES [2]. AES supports 128 bit symmetric block message and uses 128,192,256 bit key. It is restricted space environment and depending on precipitation. AES is more costly in hardware implementation. It is difficult to identify Brute-Force Attack [4]. Triple DES algorithm takes longer period of time to run encryption and decryption. It does not provide efficient software code. It has three times as many rounds as DES and it is slower. It uses 64 bit block size and it is reasonable for long term use.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

III. PROPOSED SYSTEM

VG-1 is a proposed model in internet security. It is introduced by Vani and Gayatri. VG-1 provides high security algorithm with a key size is greater than 1024 bits. It provides better authentication, confidentiality, and integrity and access control than RSA algorithm. The plaintext is converted into cipher text with the help of encrypted private key. VG-1 security algorithm uses four encrypted private keys during a process of conversion from plain text to cipher called as Encryption algorithm.

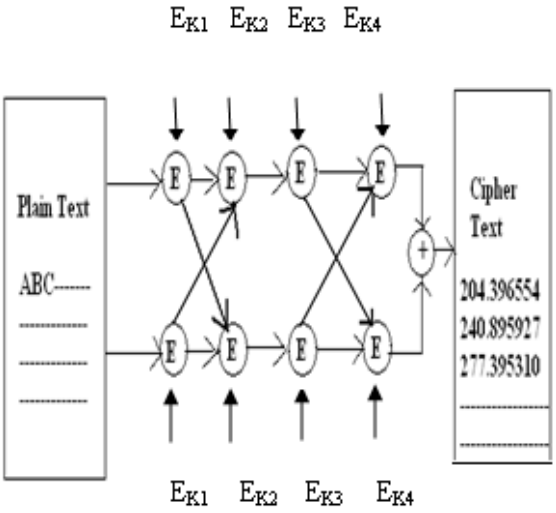

Fig 2: Basic Encryption Technique of VG-1

In this algorithm, there are four rounds for encryption. Each round requires separate Encrypted private key. Each uses different formula to encrypt data at sender site.

IV. VG-1 ENCRYPTION TECHNIQUE

VG-1 Encryption Algorithm:

Step 1: Read data from user and convert data into ASCII values of corresponding alphabets or numbers.

Step 2: ASCII values must be read and then reverse each and individual number.

Step 3: Send First numbers into Round 1 and encrypts data with encrypted private key.

Step 4: After encryption of First round, the process of second Round, third Round and fourth round is performed with help of respective encrypted private keys.

Step 5: Repeat Step1 until data of all characters or numbers sent from user is finished.

Step 6: Append all cipher text generated from each round with all encrypted private keys is sent in the network.

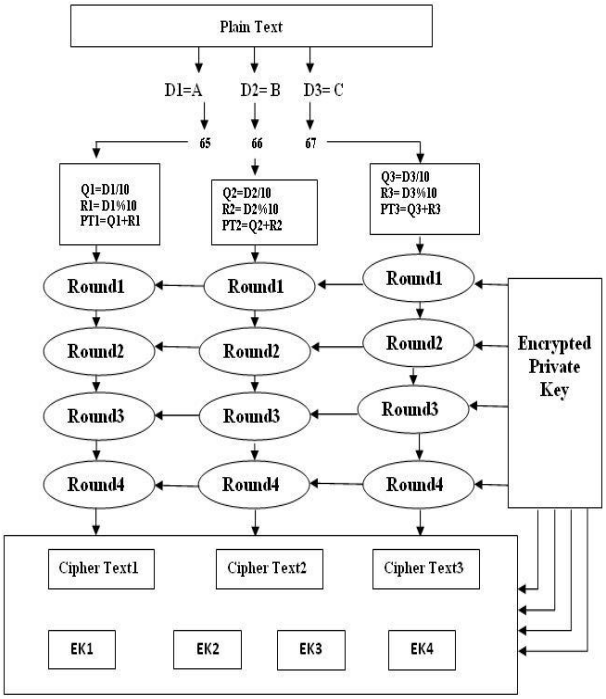

Fig 3: VG-1 Encryption technique with private keys

V. VG-1 PRIVATE KEY ENCRYPTION ALGORITHM

Step 1: The Random number generator generates three random numbers to provide an initial step for generation IR_{k1}. The IR_{k1} generates intermediate results for key1.

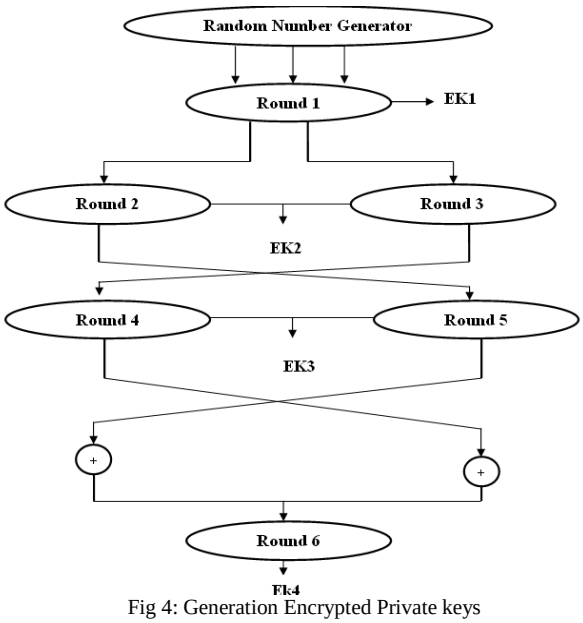

Fig 4: Generation Encrypted Private keys

Step 2: The value of 3 random numbers are sent to Round 1(R1). The round 1 apply Euler's theorem:

$$Y_1^{\,i} = Y_0 + hf(X_0, Y_0) \quad \text{..... (1)}$$

$$f(Xi, Yi) = \log_{10}\left(\frac{X0}{Y0}\right) \quad \text{.....(2)}$$

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

$$X_i = X_{i-1} + h \quad \ldots\ldots\ldots\ldots\ldots (3)$$

The result of this Round 1 is EK1 (Encrypted private key1).

Step 3: Apply result of Round 1 to Round2 and Round3. The formula applied for Round2 is:

$$\text{Sin}^3 R_1 = \frac{1}{4}[3 \text{ Sin } R_1 - \text{Sin}3R_1] \ldots\ldots\ldots (4)$$

Step 4: The formula applied for Round3 is:

$$\text{Cos}^3 R_1 = \frac{1}{4}[3 \text{ Cos } R_1 + \text{Cos}3R_1] \ldots\ldots (5)$$

$\text{Sin}^3 R_1 + \text{Cos}^3 R_1$ which results EK2 (Encrypted private key).

Step 5: Apply result from Round 3 to Round 4. The formula for Round 4 is:

$$IP_{K1} = P_3 (P_3+1) (2P_3+1)/6 \ldots\ldots (6)$$

Step 6: Apply result from Round 2 to Round 5. The formula for Round 5 is:

$$IP_{K2} = P_2^2 (P_2+1)^2 /4 \quad \ldots\ldots\ldots\ldots (7)$$

Step7: Apply XOR operation for IR_{k1} and $IR_{k2.}$

IR_{k1} ⟶ Intermediate result key 1

IR_{k2} ⟶ Intermediate result key 2

Apply result to round 6

$$IP_{\kappa 1} + IP_{\kappa 2} \longrightarrow IP_{\kappa 3} \ldots\ldots (8)$$

Step 8: In round 6, input is $IR_{k3,}$ IR_{k1} and IR_{k2}

A= IR_{k1}, B= IR_{k2}, C= IR_{k3}

Formula applied for round 6:

$$\text{SinACosB} = \frac{1}{2}[\text{Sin } (A+B) + \text{Sin } (A-B)] \ldots (9)$$

Result of round 6 is E_{p4} (Encrypted private key 1)

Example 1: assume random generator generates 10, 20, 30 is R_{n1}, R_{n2}, R_{n3}.apply VG1 encryption technique for private key.

Step1: Apply Euler's theorem

X_0=10, Y_0=20, h=30

$$F(X_{0,} Y_0) = \log_{10}(\frac{10}{20}) = - 0.301$$

$$X_1 = X_0 + h = 10 + 30 = 40$$

$$Y_1 (0) = Y_0 + hf(X_0, Y_0)$$

$$= 20 + 30(-0.301)$$

$$Y_1^{(0)} = 10.97$$

Euler's Theorem First Iteration:

$$Y_1^{(1)} = Y_0 + \frac{h}{2}[f(X_{0,} Y0) + f(X_1, Y_1^{(1)})]$$

$$= 20 + 15[(0.301) + (1 + \frac{Y_1^{(0)}}{X_1})]$$

$$= 20 + 15[-0.301 + \log_{10}\frac{40}{10.97}]$$

$$Y_1^{(1)} = 8.347$$

Euler's Theorem Second Iteration:

$$Y_1^{(2)} = Y_0 + \frac{h}{2}[f(X_{0,} Y_0) + f(X_1, Y_1^{(0)})]$$

$$Y_1^{(2)} = 25.6929$$

Therefore E_{k1}=**25.6929**

Result of Euler's theorem is applied to Round2.

Step2: calculate round 2 using following formula:

$$\text{Sin}^3 R_1 = 1/4[3\text{sin}R_1 - \text{sin}3R_1]$$

$$= 1/4[3\text{sin } (25.6929) - \text{sin}3 (25.6929)]$$

$$\text{Sin}^3 R_1 = -0.011 = R_2$$

Step3: calculate round 3 using following formula:

$$\text{cos}^3 R_1 = 1/4[3\text{cos}R_1 - \text{cos}3R_1]$$

$$\text{cos}^3 R_1 = 1/4[3\text{cos } (25.6929) - \text{cos}3 (25.6929)]$$

$$\text{cos}^3 R_1 = 7.09 = R_3$$

Result of $R_2 + R_3 =$ – (0.011) +7.09 =7.07

E_{k2} = 7.07

Step 4: calculate round 4 using following formula:

$$R_3 (R_3+1) (2 R_3+1)/6 = IR_{k1}$$

$$IR_{k1} = 135.7229 \quad \ldots\ldots\ldots\ldots (1)$$

Step 5: calculate round 5 using following formula:

$$IR_{k2} = R_2^2 (R_2+1)^2/4$$

$$IR_{k2} = -2.9588 \text{ X } 10^{-5} \ldots\ldots\ldots (2)$$

Step 6: $IR_{k3} = IR_{k1} + IR_{k2}$

$$IR_{k3} = 135.72287 = E_{k3}$$

Step7: calculate round 6 using following formula:

$$\text{SinACosB} = \frac{1}{2}[\text{Sin } (A+B) + \text{Sin } (A-B)] + IR_{k3}$$

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

E_{P4}=135.13287= E_{k4} (Encrypted private key).

Encrypted Private keys		
E_{k1}	⟶	25.6929
E_{k2}	⟶	7.07
E_{k3}	⟶	135.72287
E_{k4}	⟶	135.13287

Table 1: Generation of Private Keys

Example 2: using VG-1 security algorithm apply encryption technique for message ABC
Let us consider Alphabet

A
↓
65
↓
56

[Reverse numbers from right to left and Left to right]

$$C_T = E_{k4}(E_{k3}(E_{k2}(E_{k1}(P_T))))$$
$$P_T = D_{K1}(D_{K2}(D_{K3}(D_{K4}(C_T))))$$

Where C_T means cipher text and
P_T means plain text

Steps for VG-1 Encryption

Step1: $P_T \longrightarrow 56$
$E_{k1}(P_T) \longrightarrow IR_1$

IR_1 is intermediate result

$E_{k1\ is}$ encrypted key1

$IR_1 = 56 * 25.6929 = 1438.8024$

Step 2: $E_{k2}(IR_1) \longrightarrow IR_2$
$IR_2 = 1438.8024 \% 7.07$
$IR_2 = 203.50811$

Step 3: $E_{k3}(IR_2) \longrightarrow IR_3$
$IR_3 = 135.7228 * 203.50811 = 27620.69$

Step 4: $E_{k4}(IR_3) \longrightarrow IR_4$
$IR_4 = 27620.69 \% 135.13287$
$IR_4 = 204.3965447$

Here IR_4 is cipher text
Same steps are repeated for B & C alphabets

Plain text	Cipher text
A	204.396544
B	240.895927
C	277.395310

Table 2: Generation of Cipher Text

Position of key values inserted in cipher text:

$(R_{n1} + R_{n2} + R_{n3})/3 = (10+20+30)/3$

$(R_{n1} + R_{n2} + R_{n3})/3 = 20$ (separate individual number and add 2 numbers)

$(R_{n1} + R_{n2} + R_{n3})/3 = 2+0= 2$

In 2nd position all keys are inserted

position	Plain text	Cipher text
First position	' A '	204.396544
Second position	E_{K1}	25.6929
Third position	E_{K2}	7.07
Fourth position	E_{K3}	135.72287
Fifth position	E_{K4}	135.13287
Sixth position	'B'	240.895927
Seven position	'C'	277.395310

Table 3: Position of Encrypted private key inserted to cipher text

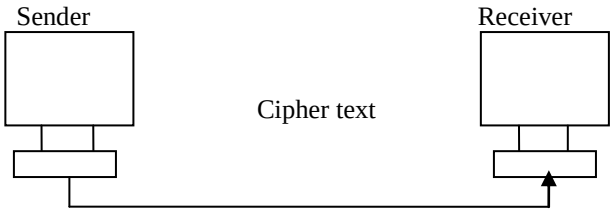

Fig 5: Transmission of cipher text

VI. VG-1 DECRYPTION TECHNIQUE

The VG-1 Decryption technique receives cipher text from sender site:

$$P_T = D_{K1}(D_{K2}(D_{K3}(D_{K4}(C_T))))$$

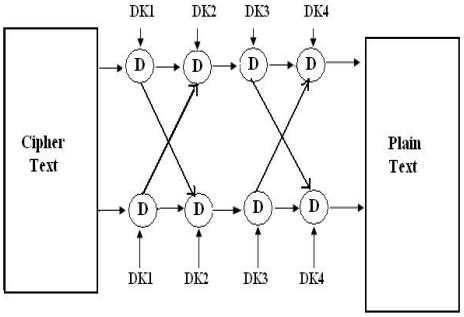

Fig 6: VG-1 Decryption Technique

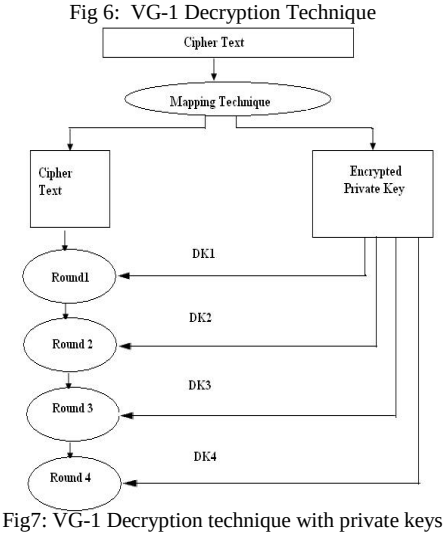

Fig7: VG-1 Decryption technique with private keys

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

VG-1 Decryption Algorithm:

Step1: using first digit number, identify position of key value inserted based in mapping technique

Step 2: Differentiate key values and original data.

Step 3: identify D_{k1}, D_{k2}, D_{k3}, D_{k4}.

Step 4: Use mapping technique to identify cipher text and encrypted private keys.

Cipher Text	Private key
204.396544	25.6929
	7.07
240.895927	135.72287
277.395310	135.13287

Table 4: Generation of Cipher text and private key

Step 5: Identify First number and read the value of cipher text and apply formula:

$$IR_1 = D_{k4}(C_T)$$

IR_1 = 204.396544 /135.13287
IR_1 = 27620.6916 ……..…….. (1)

Step 6: $IR_2 = D_{k3}(IR_1)$

IR_2 =27620.6916 /135.72287

IR_2 = 203.50801 ……..... (2)

Step 7: $IR_3 = D_{k2}(IR_2)$

IR_3 = 203.50801* 7.07

IR_3 = 1438.801631…… (3)

Step 8: $IR_4 = D_{k1}(IR_3)$

IR_4 =1438.801631/25.6929

IR_4 = 55.9999 …… (4)

$IR_4 \approx 56$

Step 9: Reverse the number sent from IR_4

Hence result is 65.

Cipher Text	Scrambled number	ASCII value	Plain text
204.396544	56	65	A
240.8959277	66	66	B
277.395310	76	67	C

Table 5: Decrypted cipher text to plain text

VII. COMPARATIVE ANALYSIS

Algorithm	Clock cycles Per Round	Number of Rounds	No of Clock cycles per Bytes Encrypted
Bluefish	9	16	18
RC5	12	16	23
DES	18	16	45
Triple DES	18	48	108
RSA	15	10	18
VG-1	20	18	78

Table 6: Comparative Analysis on clock cycles

Algorithm	Encryption /Decryption	Digital Signature	Key Exchange
RSA	YES	YES	YES
DES	YES	YES	YES
AES	YES	YES	YES
Triple DES	YES	YES	YES
Diffie-Hellman	NO	NO	YES
VG-1	YES	YES	YES

Table 7: Comparative techniques for encryption and decryption

VIII. RESULTS AND DISCUSSION

VG-1 security algorithm performs efficient technique for encryption and decryption. It provides high security on cipher text. The opponent will be able to identify which is correct key and which is cipher text. A VG-1 result provides high performance and less delay and very complex technique to identify plain text by attacker.

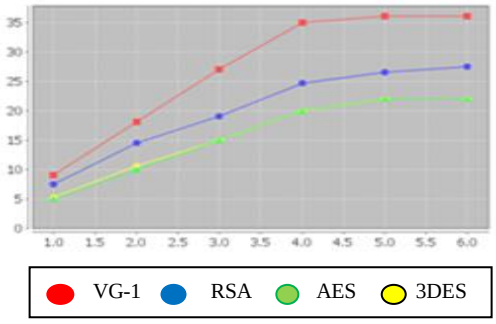

Fig 8: Comparison on Performance of different security Algorithms

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

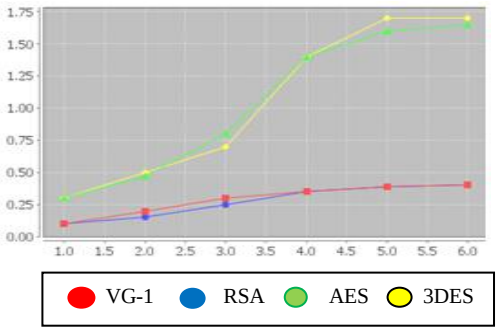

Fig 9: Processing Delay of Different security Algorithms

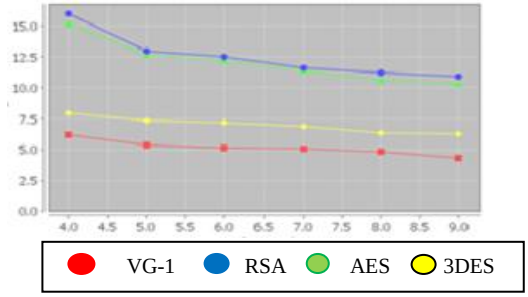

Fig 10: Processing Time of Different security Algorithms

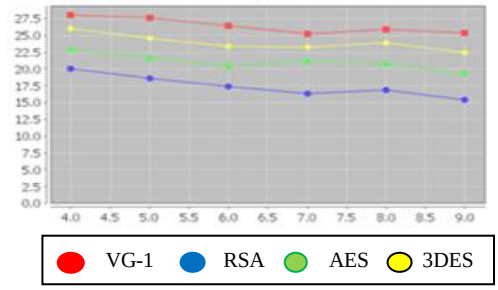

Fig 11: Complexity of Encryption and Decryption Techniques Of security Algorithms by attacker

IX. CONCLUSION

In this paper, we propose VG-1 Security algorithm provides high security for data transmission. This algorithm is more useful for current technologies such as online exam, online banking, online ticket reservations, online shopping, online business transaction needs and online ATM transactions. VG-1 security algorithm provides greater efficiency on identifying all possible attacks such as Masquerade, content modification, sequence modification, timing modification, source repudiation and data repudiation. VG-1 algorithm at receiver site identifies Brute-Force attack. For attacker, it is very different to identify plain text from cipher text and difficult for attacker to identify from cipher text which data is encrypted private key and which data is cipher text.

REFERENCES

[1] D.Sharmila, Dr. R. Neelavani,"Performance Analysis of SAFER+ and Triple DES security algorithm for Blurtooth security system," IJCSNS, Sathyamangalam, Coimbatore, Tamil Nadu, Vol .9 No.2, Feb 2009.

[2] Neha Jain, Gurpret Kaur,"Implementing DES Algorithm in cloud for data security," VSRD-IJCSIT, vol.2 (4), pp316-321, Feb 2012.

[3] Nimmi Gupta,"Implementation of optimized DES Encryption Algorithm upto 4 Round on Sparatan3," IJCTEE, sehore, madhyapradesh Vol 2, Issue1, ISSN-2249-6343.

[4] Gohil Rikitaben Karasanbhai,Mary Grace Shajan,"AES Algorithm for Secured Wireless Communication," National conference on recent trends in engineering and technology,vadodara,India.

[5] Niels Ferguson," AES – CBC + Elephant diffuser a disk encryption algorithm for windows vista," Microsoft, Aug2006.

[6] Majithia schin, Dinesh Kumar,"Implementation and Analysis of AES, DES and Triple DES on GSM networks," IJCSNS,Vol 10 No.1,Jalandhar,India,Jan 2010.

BIOGRAPHIES

VANI .N M.TECH,

The author VANI .N is from native from Bellary District of Karnataka, India. This author completed M.Tech in Computer Networking form AMC Engineering College. She is working as Assistant Professor of CSE department in RYMEC college of Engineering and Technology, Bellary, for the past Three years. Her area of interest includes Cloud Computing.

SREELATHA.P.K MTECH

The author SREELATHA.P.K is from Bangalore District of Karnataka, India. She completed M.Tech in Computer Science from NMIT, Bangalore. She is working as Assistant Professor of CSE department in SVIT Engineering College, Bangalore, having 6 years of Experience. Her area of interest includes Cloud Computing, image processing.

PARVATHY.S MTECH

The author, PARVATHY.S has completed M.Tech in Computer Network Engineering from AMC Engineering College. She is currently working as an Assistant Professor of ISE department in AMC college of Engineering and Technology, Bangalore having 3 years of Experience. Her area of interest includes Cloud Computing and Computer networks. She hails from Trivandrum, District of Kerala, India.